ShareTech UTM Solution

Website
www.sharetech.com.tw/en-us

Sales Info
sales@sharetech.com.tw

Tech Support
help@sharetech.com.tw

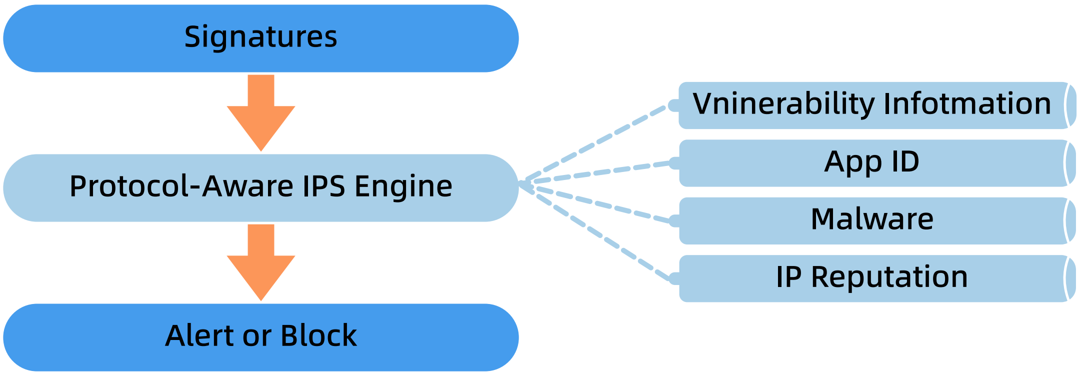
IPS Defends Against Dynamic Cyber Attacks

IPS (Intrusion Prevention System) is an active defense technology that uses signature-based detection to compare against a database and identify potential vulnerabilities and attack behaviors within a network. Some systems and applications often contain unpatched vulnerabilities, which attackers may exploit to disrupt operations or gain control over applications and devices.

Thus, the primary role of IPS is to reinforce firewall security by addressing gaps that firewalls might not completely block. It ensures system security through real-time detection and interception of malicious access attempts, preventing potential damage.

- Proactively identifies and blocks attacks such as brute-force attacks, SQL injection, and XSS attacks.
- Intercepts malicious traffic by detecting anomalies and immediately blocking attack sources, reducing the impact of threats.
- Enhances firewall protection across multiple OSI layers, covering the application layer (Layer 7), transport layer (Layer 4), and network layer (Layer 3)

IPS(Intrusion Prevention System)



Signatures

Protocol-Aware IPS Engine

Alert or Block

Vninerability Infotmation

App ID

Malware

IP Reputation

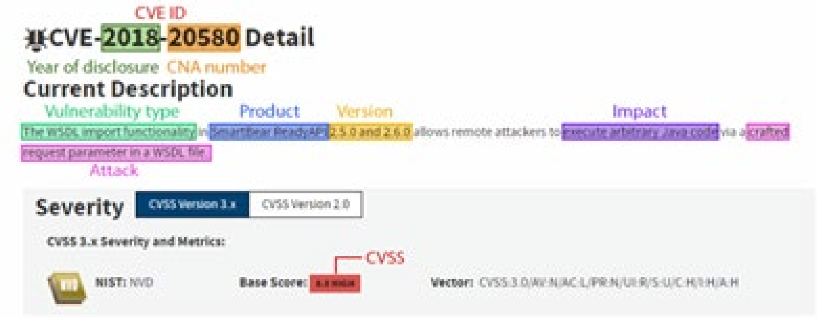
ShareTech Adjusts the CVE Strategy to the New Reality Units are recommended to inspect devices on every gate to see if the related CVEs have been patch. CVE numbers are added in the IPS signatures, which allows admins to block or log signatures based on CVE IDs.

CVE ID (CVE-YEAR-XXXX)

Vulnerabilites vs Exposures

	Vulnerabilities	Exposures
Definition	a flaw in softqare code	a mistake in software code or configuratiin
Purpose	access to the system	access to the system
Method	• pose as a legitimate user • execute code • install malware	• stay on the dark web • steal data, certificatrs, and PPI.

Common Vulnerabilities and Exposures (CVE) system provides a standardized way to identify and catalog known security vulnerabilities and exposures in software and hardware.



CVE-2018-20580 Detail

Current Description

The WSDL import functionality in SmartBear ReadyAPI 2.5.0 and 2.6.0 allows remote attackers to execute arbitrary Java code via a crafted request parameter in a WSDL file

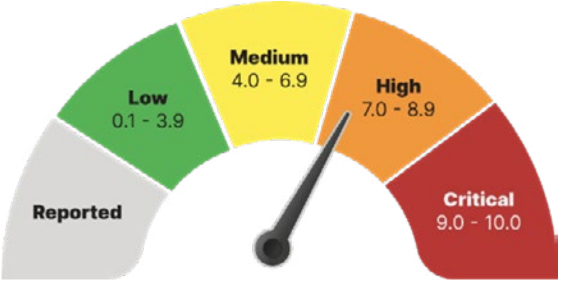
Severity

CVSS 3.x Severity and Metrics:

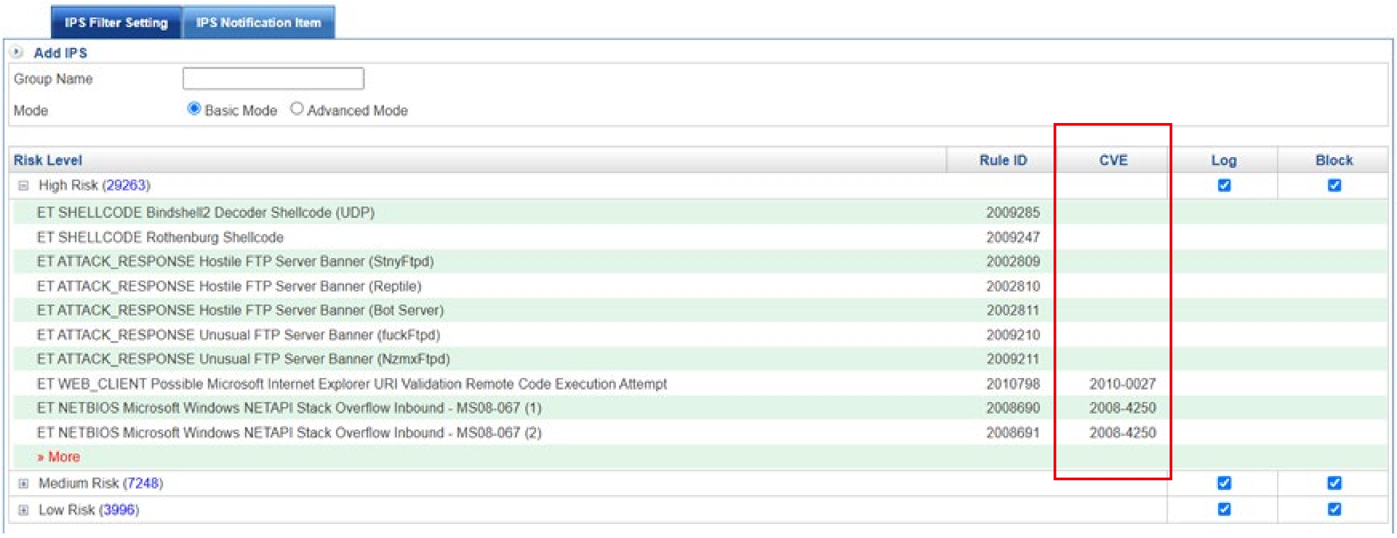
NIST: NVD

Base Score:

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



ShareTech Next Generation UTM Interface:



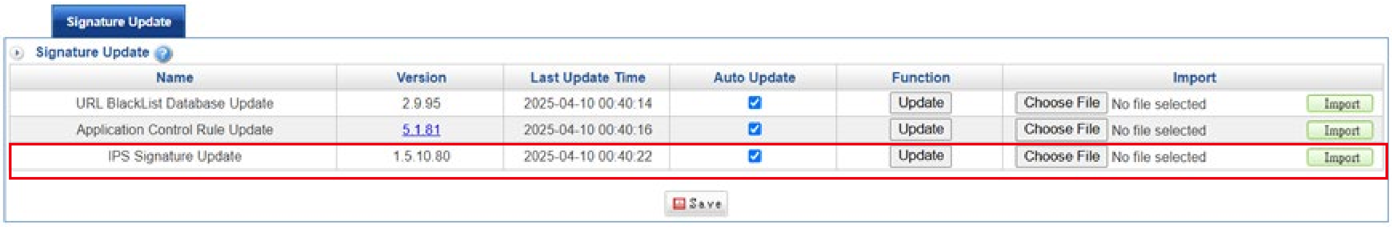
Add IPS

Group Name

Mode ● Basic Mode ○ Advanced Mode

Risk Level	Rule ID	CVE	Log	Block
⊟ High Risk (29263)			☑	☑
ET SHELLCODE Bindshell2 Decoder Shellcode (UDP)	2009285			
ET SHELLCODE Rothenburg Shellcode	2009247			
ET ATTACK_RESPONSE Hostile FTP Server Banner (StnyFtpd)	2002809			
ET ATTACK_RESPONSE Hostile FTP Server Banner (Reptile)	2002810			
ET ATTACK_RESPONSE Hostile FTP Server Banner (Bot Server)	2002811			
ET ATTACK_RESPONSE Unusual FTP Server Banner (fuckFtpd)	2009210			
ET ATTACK_RESPONSE Unusual FTP Server Banner (NzmxFtpd)	2009211			
ET WEB_CLIENT Possible Microsoft Internet Explorer URI Validation Remote Code Execution Attempt	2010798	2010-0027		
ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (1)	2008690	2008-4250		
ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (2)	2008691	2008-4250		
» More				
⊞ Medium Risk (7248)			☑	☑
⊞ Low Risk (3996)			☑	☑

Ensure regular updates of IPS signature databases.



Signature Update

Name	Version	Last Update Time	Auto Update	Function	Import
URL BlackList Database Update	2.9.95	2025-04-10 00:40:14	☑	Update	Choose File No file selected Import
Application Control Rule Update	5.1.81	2025-04-10 00:40:16	☑	Update	Choose File No file selected Import
IPS Signature Update	1.5.10.80	2025-04-10 00:40:22	☑	Update	Choose File No file selected Import